CLIENT UPDATE

MANAGING CYBERSECURITY RISKS ARISING FROM AI

A fundamental piece of guidance on assessing cybersecurity risk associated with the use of AI was issued by the New York State Department of Financial Services ("NYDFS") on October 16 (the "Guidance"). While the Guidance applies to entities regulated by the NYDFS it provides valuable guidance to all companies for managing the new cybersecurity risks associated with AI.

Companies will need to decide how best to integrate their general cybersecurity risk-management programs with their general AI-risk management programs to make sure AI-related cybersecurity risks are properly addressed.

Guidance on Risks

The Guidance divides cybersecurity-related AI risks into two categories: (1) risks caused by threat actors' use of AI; and (2) risks caused by companies' use of (or reliance on) AI.

Risks from Threat's Actors' use of AI. AI-Enabled Social Engineering: Threat actors are increasingly using AI to create realistic and interactive audio, video, and text ("deepfakes") that allow them to target specific individuals via email (phishing), telephone (vishing), text (SMiShing), videoconferencing, and online postings. These AI-driven attacks often attempt to convince employees to divulge sensitive information about themselves and their employers or wiring substantial amounts of funds to fraudulent accounts.

AI-Enhanced Cybersecurity Attacks: Another major risk associated with AI is the ability of threat actors to amplify the potency, scale, and speed of existing types of cyberattacks. As AI can scan and analyze vast amounts of information much faster than humans, threat actors can use AI quickly and efficiently to identify and exploit security vulnerabilities, often allowing threat actors to access more Information Systems at a faster rate.

Risks from Companies' Use of AI. Exposure or Theft of Vast Amounts of Nonpublic Information: Use of AI by companies will often involve the collection and processing of large volumes of nonpublic information, providing more opportunities for attackers and creating more data, devices, and locations for companies to protect. Additionally, the data used in AI applications sometimes contains biometric data, such as faceprints or fingerprints, which a threat actor can leverage to bypass

MFA (Multi-factor Authentication) and gain access to additional information systems.

Increased Vulnerabilities Due to Third-Party, Vendor Dependencies: Cyber-related AI risks are further compounded by companies' heavy reliance on third-party service providers (who are vulnerable to cyberattacks) to provide them with AI tools and/or the data used to train and operate them.

Guidance on Mitigation Measures

The Guidance provides examples of controls that will help companies reduce their AI-related cybersecurity risks:

- Ensure risk assessments account for AI-specific risks, including for third-party service providers.
- Conduct incident response planning, testing, and training to account for AI related incidents, and ensure that such preparedness be tested, and that relevant personnel be appropriately informed about AI-related cybersecurity risks, including a Cross-functional committee, boards and senior leadership.
- The Guidance recommends that due diligence of third-party service providers should include diligence on the AI-related risks they pose to themselves and to the companies.
- The Guidance reinforces the focus on MFA as a critical measure to combat cyberattacks.
- All personnel should be trained on the risks posed by AI, including procedures adopted by the organization to mitigate risks related to AI, and responses to AI-enhanced social engineering attacks.
- Given the large amounts of data that are often used to operate AI systems, the Guidance further underscores the need for companies to implement data minimization practices.

Companies are likely to be made subject to specific rules issued by Mexican regulators. However, the mapping of the above-mentioned steps, will put them in the front row of the starting line, when such rules are issued.

* * *

Please do not hesitate to contact us with any questions.

Berdeja Abogados, S.C.

November 5, 2024